

This listing of claims will replace all prior versions, and listings, of claims in the application:

Amendments to the Claims:

Claim 1. (currently amended): A method for forming a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer-~~wherein said data segments are grouped irrespective of their original order;~~

forming a first segment checksum for each said data segment;

forming said first commutative checksum by a commutative operation on said first segment checksums; and

cryptographically protecting said first commutative checksum by using a cryptographic operation.

Claim 2. (currently amended): A method for checking a predetermined cryptographic commutative checksum comprising the steps of:

grouping digital data into a number of data segments by a computer-~~wherein said data segments are grouped irrespective of their original order;~~

allocating said predetermined cryptographic checksum to said digital data;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum;

forming a second segment checksum for each said data segment;

forming a second commutative checksum by a commutative operation on said second segment checksums; and

checking said second commutative checksum for a match with said first commutative checksum.

Claim 3. (currently amended): A method for forming and checking a first commutative checksum for digital data comprising the steps of:

grouping said digital data into a number of data segments by a computer, ~~wherein said data segments are grouped irrespective of their original order;~~

forming a first segment checksum for each said data segment;

forming said first commutative checksum by a commutative operation on said first segment checksums;

cryptographically protecting said first commutative checksum by using at least one cryptographic operation, which forms a cryptographic commutative checksum;

subjecting said cryptographic commutative checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum;

forming a second segment checksum for each said data segment of said digital data to which said first commutative checksum is allocated;

forming a second commutative checksum by a commutative operation on said second segment checksums; and

checking said second commutative checksum for a match with said reconstructed first commutative checksum.

Claims 4-9 (canceled).

Claim 10. (currently amended): An arrangement for forming a first commutative checksum for digital data which are grouped into a number of data segments, said arrangement comprising:

an arithmetic and logic unit,

a first segment checksum, which is formed for each said data segment ~~irrespective of each data segment's original order,~~

a commutative operation which forms said first commutative checksum by operating on said segment checksums, and

a cryptographic operation which cryptographically protects said first commutative checksum.

Claim 11. (previously presented): An arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

- an arithmetic and logic unit;

- an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation;

- a second segment checksum which is formed for each said data segment, wherein said second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function;

- a commutative operation which operates on said second segment checksums which forms a second commutative checksum; and

- a comparator which checks for a match between said second commutative checksum and said first commutative checksum.

Claim 12. (previously presented): An arrangement for forming and checking a first commutative checksum for digital data which is grouped into a number of data segments, said arrangement comprising:

- an arithmetic and logic unit,

- a first segment checksum, which is formed for each said data segment,

- a commutative operation which forms said first commutative checksum by operating on said first segment checksums,

- a cryptographic operation which cryptographically protects said first commutative checksum,

- a cryptographic commutative checksum formed by said cryptographic operation,

- an inverse cryptographic operation to form a first commutative checksum from said cryptographic commutative checksum,

- a second segment checksum which is formed for each said data segment of said digital data to which said first commutative checksum is allocated,

- a commutative operation which operates on said second segment checksums which forms a second commutative checksum, and

a comparator which checks for a match between said second commutative checksum and a reconstructed first commutative checksum, wherein said first and second segment checksum are formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function.

Claims 13-18. (canceled).

Claim 19. (previously presented): A method according to claim 1, further comprising the step of:

forming said first segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 20. (previously presented): A method according to claim 2, further comprising the step of:

forming said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 21. (previously presented): A method according to claim 3, further comprising the step of:

forming said first segment checksums and said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 22. (previously presented): A method according to claim 1, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 23. (previously presented): A method according to claim 2, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 24. (previously presented): A method according to claim 3, wherein:
said cryptographic operation is an operation selected from the group consisting of a
symmetric cryptographic method and an asymmetric cryptographic method.

Claim 25. (previously presented): A method according to claim 1, wherein:
said commutative operation exhibits the property of associativity.

Claim 26. (previously presented): A method according to claim 2, wherein:
said commutative operation exhibits the property of associativity.

Claim 27. (previously presented): A method according to claim 3, wherein:
said commutative operation exhibits the property of associativity.

Claim 28. (previously presented): A method according to claim 1, wherein said
digital data and the first cryptographic, commutative checksum are archived.

Claim 29. (previously presented): A method according to claim 2, wherein said
digital data and the prescribed cryptographic commutative checksum have been archived.

Claim 30. (previously presented): A method according to claim 3, wherein said
digital data are secured which are processed corresponding to a network management protocol.

Claim 31. (previously presented): A method according to claim 1, further
comprising the steps of:
protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claim 32. (previously presented): A method according to claim 2, further
comprising the steps of:

protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claim 33. (previously presented): A method according to claim 3, further comprising the steps of:

protecting said digital data; and
processing said digital data in accordance with a network management protocol.

Claim 34. (previously presented): An arrangement according to claim 10, wherein:
said first segment checksums are formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Claim 35. (canceled):

Claim 36. (currently amended): An arrangement according to claim 11, wherein:
~~said a~~ first segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function.

Claim 37. (previously presented): An arrangement according to claim 10, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 38. (previously presented): An arrangement according to claim 11, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 39. (previously presented): An arrangement according to claim 12, wherein:
said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Claim 40. (previously presented): An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 41. (previously presented): An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 42. (previously presented): An arrangement according to claim 12, wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Claim 43. (previously presented): An arrangement according to claim 10, wherein: said digital data and the first cryptographic, commutative checksum are archived.

Claim 44. (previously presented): An arrangement according to claim 11, wherein: said digital data and the prescribed cryptographic commutative checksum have been archived.

Claim 45. (previously presented): An arrangement according to claim 12, wherein: said digital data and the first cryptographic, commutative checksum are archived.

Claim 46. (previously presented): An arrangement according to claim 10, wherein: said digital data are protected via an arrangement of said arithmetic and logic unit; and said digital data are processed in accordance with a network management protocol.

Claim 47. (previously presented): An arrangement according to claim 11, wherein: said digital data are protected via an arrangement of said arithmetic and logic unit; and said digital data are processed in accordance with a network management protocol.

Claim 48. (previously presented): An arrangement according to claim 12, wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit; and
said digital data are processed in accordance with a network management protocol.